AMENDMENTS TO THE CLAIMS

Pursuant to 37 C.F.R. § 1.121 the following listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of the Claims

1 – 4. (Canceled).

5. (Currently Amended) A method for establishing a common key for a group of at least three subscribers for transmitting messages over a communication channel, the method comprising the steps of:

generating, by each subscriber T_j, a respective message $N_j = (g^{zj} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zj, j = 1 to n, where n is the number of subscribers in the group of at least three subscribers;

sending the respective message N_j, by each subscriber, to each of the other subscribers T_i[[,]];

encrypting, by a first subscriber T_1, the received messages N_j of the other subscribers T_j, $j \neq 1$, with the random number z1 to form a respective transmission key k^{1j} for each subscriber T_j, $j \neq 1$;

computing, by each subscriber T_j, $j \neq 1$, a symmetrical counterpart k^{j1} of the respective transmission key k^{1j} using the received message N_1;

sending, by the first subscriber T_1, the random number z1 to all other subscribers T_j, $j \neq 1$ in encrypted form by generating a message M_{1j} according to $M_{1j} := E(k^{1j}, z1)$, $E(k^{1j}, z1)$ being a symmetrical encryption algorithm in which the random number z1 is encrypted with the transmission key k^{1j};

decrypting, by each subscriber T_j, the message M_{1j};

determining a common key k, by each subscriber Tj, using an assignment $k := h(z1, g^{z2}, ..., g^{zn})$, $h(x1, x2, ..., xn)$ being a function which is symmetrical in the arguments x2, ..., xn;

encrypting, by one of the subscribers T_i, a transmission message using the common key k; and

transmitting the encrypted transmission message to at least one of the other subscribers T_j, $j \neq i$.

6. (Currently Amended) The method as recited in claim 5 wherein the transmission key is known to each subscriber T_j according to $k^{1j} = k^{j1}$.

7. (Previously Presented) A method for establishing a common key for a group of subscribers for encryption and decryption of messages, the method comprising the steps of:

each of the subscribers T_j generating a respective random number zj, where j goes from 1 to n and n is the number of subscribers in the group of subscribers;

each of the subscribers T_j generating a respective first message $N_j = (g^{zj} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G;

each of the subscribers T_j sending the respective first message N_j to each of the other subscribers T_j;

a first subscriber T_1 computing a transmission key $k^{1j} = N_j^{z1} \bmod p$ for each of the other subscribers T_j, $j \neq 1$ based on the received respective first message N_j, $j \neq 1$;

each of the subscribers T_j, $j \neq 1$, computing a symmetrical counterpart k^{j1} of the respective transmission key k^{1j} using the received first message N_1;

the first subscriber T_1 encrypting a second message $M_{1j} := E(k^{1j}, z1)$ for each of the other subscribers T_j, $j \neq 1$, where $E(k^{1j}, z1)$ is a symmetrical encryption algorithm in which z1 is encrypted with the transmission key k^{1j};

the first subscriber T_1 sending the encrypted second message M_{1j} to each of the other subscribers T_j, $j \neq 1$; and

each of the subscribers T_j decrypting the second message M_{1j};

each of the subscribers T_j computing a common key k according to an assignment $k:=h(z1, g^{z2}, \ldots g^{zn})$, where $h(x1,x2\ldots xn)$ is a symmetrical function;

a subscriber T_i encrypting a third message using the common key k; and

the subscriber T_i transmitting the encrypted third message to at least one of the other subscribers T_j, $j \neq i$.

8. (Previously Presented) The method according to claim 7, wherein each respective random number zj is selected from the set $\{1, \ldots p\text{-}2\}$.

9. (Previously Presented) The method according to claim 7, wherein the length of p is at least 1024 bits.

10. (Previously Presented) The method according to claim 7, wherein g has a multiplicative order of at least 2^{160}.

11. (Currently Amended) The method according to claim 7 wherein the transmission key is known to [[a]]<u>each</u> respective subscriber ~~Tj~~ <u>T_j</u> according to $k^{1j} = k^{j1}$.

12. (Previously Presented) The method according to claim 7, wherein $h(z1, g^{z2}, \ldots g^{zn}) = g^{z1*z1} * g^{z2*z1} * \ldots g^{zn*z1}$.

13. (Previously Presented) A method for establishing a common key for a group of subscribers for encryption and decryption of messages, the method comprising the steps of:

each of the subscribers T_j generating a respective random number zj, where j goes from 1 to n and n is the number of subscribers in the group of subscribers;

each of the subscribers T_j storing the respective random number zj in a respective memory;

each of the subscribers T_j generating a respective first message $N_j = (g^{zj} \bmod p)$ from a publicly known element g of large order of a publicly known mathematical group G;

each of the subscribers T_j sending the respective first message $N_j, j \neq 1$ to each of the other subscribers T_j;

the first subscriber T_1 storing each of the received first messages $N_j, j \neq 1$ in a memory;

the first subscriber T_1 computing a transmission key $k^{1j} = N_j^{z1} \bmod p$ for each of the other subscribers $T_j, j \neq 1$, based on the received respective first message $N_j, j \neq 1$;

each of the subscribers $T_j, j \neq 1$, computing a symmetrical counterpart k^{j1} of the respective transmission key k^{1j} using the received first message N_1;

the first subscriber T_1 encrypting a second message $M_{1j} := E(k^{1j}, z1)$ for each of the other subscribers T_j, $j \neq 1$, where $E(k^{1j}, z1)$ is a symmetrical encryption algorithm in which z1 is encrypted with the transmission key k^{1j} ;

the first subscriber T_1 sending the encrypted second message M_{1j} to each of the respective other subscribers T_j, $j \neq 1$;

each of the respective other subscribers T_j, $j \neq 1$, storing the received encrypted second message in the respective memory; and

each of the subscribers T_j decrypting the second message M_{1j};

each of the subscribers Tj computing a common key k according to an assignment $k:=h(z1, g^{z2}, \ldots g^{zn})$, where h(x1,x2...xn) is a symmetrical function, and n is the number of subscribers in the group;

one of the subscribers T_i encrypting a third message using the common key k; and

the subscriber T_i transmitting the encrypted third message to at least one of the other subscribers T_j, $j \neq i$.

14. (Previously Presented) The method according to claim 13, whereby a maximum number of transmission rounds required is two.

15. (Previously Presented) The method according to claim 13, further comprising the steps of:

the subscriber T_i transmitting the encrypted third message to each of the other respective subscribers T_j, $j \neq i$;

each of the other respective subscribers T_j, $j \neq i$ decrypting the received encrypted third message using the computed common k.

16. (Previously Presented) The method according to claim 5, further comprising the step of:

decrypting, by the at least one of the other subscribers T_j, $j \neq i$, the transmitted transmission message using the common key k.

17. (Previously Presented) The method according to claim 7, further comprising the step of:

the at least one other subscriber T_j, $j \neq i$ decrypting the received third message using the common key k.

18. (Previously Presented) The method according to claim 13, further comprising the step of:

the at least one other subscriber T_j, $j \neq i$ decrypting the received third message using the common key k.